

# EXHIBIT 6



# **CIS Apple iOS 13 and iPadOS 13 Benchmark**

v1.0.0 - 11-12-2019

# Terms of Use

Please see the below link for our current terms of use:

<https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/>

## Table of Contents

Terms of Use .....	1
Overview .....	7
Intended Audience .....	7
Consensus Guidance.....	7
Typographical Conventions .....	9
Scoring Information .....	9
Profile Definitions .....	10
Acknowledgements .....	11
Recommendations .....	12
1 Benchmark Guidance .....	12
2 Configuration Profile Recommendations for End-User Owned Devices.....	13
2.1 General .....	14
2.1.1 (L1) Ensure a 'Consent Message' has been 'Configured' (Scored).....	14
2.1.2 (L1) Ensure 'Controls when the profile can be removed' is set to 'Always' (Scored) .....	16
2.2 Restrictions.....	18
2.2.1 Functionality.....	19
2.2.1.1 (L1) Ensure 'Allow voice dialing while device is locked' is set to 'Disabled' (Scored) .....	19
2.2.1.2 (L1) Ensure 'Allow Siri while device is locked' is set to 'Disabled' (Scored) .....	21
2.2.1.3 (L1) Ensure 'Allow managed apps to store data in iCloud' is set to 'Disabled' (Scored) .....	23
2.2.1.4 (L1) Ensure 'Force encrypted backups' is set to 'Enabled' (Scored).....	25
2.2.1.5 (L2) Ensure 'Allow users to accept untrusted TLS certificates' is set to 'Disabled' (Scored) .....	27
2.2.1.6 (L1) Ensure 'Allow documents from managed sources in unmanaged destinations' is set to 'Disabled' (Scored) .....	29
2.2.1.7 (L1) Ensure 'Allow documents from unmanaged sources in managed destinations' is set to 'Disabled' (Scored) .....	31

2.2.1.8 (L1) Ensure 'Treat AirDrop as unmanaged destination' is set to 'Enabled' (Scored) .....	33
2.2.1.9 (L2) Ensure 'Allow Handoff' is set to 'Disabled' (Scored) .....	35
2.2.1.10 (L1) Ensure 'Force Apple Watch wrist detection' is set to 'Enabled' (Scored) .....	37
2.2.1.11 (L1) Ensure 'Show Control Center in Lock screen' is set to 'Disabled' (Scored) .....	39
2.2.1.12 (L1) Ensure 'Show Notification Center in Lock screen' is set to 'Disabled' (Scored) .....	41
2.2.2 Apps .....	43
2.2.2.1 (L1) Ensure 'Force fraud warning' is set to 'Enabled' (Scored) .....	43
2.2.2.2 (L1) Ensure 'Accept cookies' is set to 'From websites I visit' or 'From current website only' (Scored) .....	45
2.3 Domains .....	47
2.3.1 (L1) Ensure 'Managed Safari Web Domains' is 'Configured' (Not Scored) ...	47
2.4 Passcode .....	49
2.4.1 (L1) Ensure 'Allow simple value' is set to 'Disabled' (Scored) .....	49
2.4.2 (L1) Ensure 'Minimum passcode length' is set to '6' or greater (Scored) .....	51
2.4.3 (L1) Ensure 'Maximum Auto-Lock' is set to '2 minutes' or less (Scored) .....	53
2.4.4 (L1) Ensure 'Maximum grace period for device lock' is set to 'Immediately' (Scored) .....	55
2.4.5 (L1) Ensure 'Maximum number of failed attempts' is set to '6' (Scored) .....	57
2.5 VPN .....	59
2.5.1 (L1) Ensure 'VPN' is 'Configured' (Not Scored) .....	59
2.6 Mail .....	61
2.6.1 (L1) Ensure 'Allow user to move messages from this account' is set to 'Disabled' (Scored) .....	61
2.7 Notifications .....	63
2.7.1 (L1) Ensure 'Notification Settings' are configured for all 'Managed Apps' (Not Scored) .....	63
3 Configuration Profile Recommendations for Institutionally Owned Devices .....	65
3.1 General .....	66

3.1.1 (L1) Ensure 'Controls when the profile can be removed' is set to 'Never' (Scored) .....	66
3.2 Restrictions.....	68
3.2.1 Functionality.....	69
3.2.1.1 (L2) Ensure 'Allow screenshots and screen recording' is set to 'Disabled' (Not Scored) .....	69
3.2.1.2 (L1) Ensure 'Allow voice dialing while device is locked' is set to 'Disabled' (Scored) .....	71
3.2.1.3 (L1) Ensure 'Allow Siri while device is locked' is set to 'Disabled' (Scored) .....	73
3.2.1.4 (L1) Ensure 'Allow iCloud backup' is set to 'Disabled' (Scored).....	75
3.2.1.5 (L1) Ensure 'Allow iCloud documents & data' is set to 'Disabled' (Scored) .....	77
3.2.1.6 (L1) Ensure 'Allow iCloud Keychain' is set to 'Disabled' (Scored).....	79
3.2.1.7 (L1) Ensure 'Allow managed apps to store data in iCloud' is set to 'Disabled' (Scored) .....	81
3.2.1.8 (L2) Ensure 'Allow USB drive access in Files app' is set to 'Disabled' (Scored) .....	83
3.2.1.9 (L2) Ensure 'Allow network drive access in Files app' is set to 'Disabled' (Scored) .....	85
3.2.1.10 (L1) Ensure 'Force encrypted backups' is set to 'Enabled' (Scored) .....	87
3.2.1.11 (L1) Ensure 'Allow Erase All Content and Settings' is set to 'Disabled' (Scored) .....	89
3.2.1.12 (L2) Ensure 'Allow users to accept untrusted TLS certificates' is set to 'Disabled' (Scored) .....	91
3.2.1.13 (L1) Ensure 'Allow installing configuration profiles' is set to 'Disabled' (Scored) .....	93
3.2.1.14 (L1) Ensure 'Allow adding VPN configurations' is set to 'Disabled' (Scored) .....	95
3.2.1.15 (L2) Ensure 'Allow modifying cellular data app settings' is set to 'Disabled' (Scored) .....	97
3.2.1.16 (L1) Ensure 'Allow USB accessories while the device is locked' is set to 'Disabled' (Scored) .....	99

3.2.1.17 (L2) Ensure 'Allow pairing with non-Configurator hosts' is set to 'Disabled' (Scored) .....	101
3.2.1.18 (L1) Ensure 'Allow documents from managed sources in unmanaged destinations' is set to 'Disabled' (Scored) .....	103
3.2.1.19 (L1) Ensure 'Allow documents from unmanaged sources in managed destinations' is set to 'Disabled' (Scored) .....	105
3.2.1.20 (L1) Ensure 'Treat AirDrop as unmanaged destination' is set to 'Enabled' (Scored) .....	107
3.2.1.21 (L1) Ensure 'Allow Handoff' is set to 'Disabled' (Scored).....	109
3.2.1.22 (L1) Ensure 'Require Touch ID / Face ID authentication before AutoFill' is set to 'Enabled' (Scored) .....	111
3.2.1.23 (L1) Ensure 'Force Apple Watch wrist detection' is set to 'Enabled' (Scored) .....	113
3.2.1.24 (L1) Ensure 'Allow setting up new nearby devices' is set to 'Disabled' (Scored) .....	115
3.2.1.25 (L1) Ensure 'Allow proximity based password sharing requests' is set to 'Disabled' (Scored) .....	117
3.2.1.26 (L1) Ensure 'Show Control Center in Lock screen' is set to 'Disabled' (Scored) .....	119
3.2.1.27 (L1) Ensure 'Show Notification Center in Lock screen' is set to 'Disabled' (Scored) .....	121
3.2.2 Apps .....	123
3.2.2.1 (L1) Ensure 'Force fraud warning' is set to 'Enabled' (Scored) .....	123
3.2.2.2 (L1) Ensure 'Accept cookies' is set to 'From websites I visit' or 'From current website only' (Scored) .....	125
3.3 Domains .....	127
3.3.1 (L1) Ensure 'Managed Safari Web Domains' is 'Configured' (Not Scored).127	
3.4 Passcode .....	129
3.4.1 (L1) Ensure 'Allow simple value' is set to 'Disabled' (Scored).....	129
3.4.2 (L1) Ensure 'Minimum passcode length' is set to '6' or greater (Scored) ...	131
3.4.3 (L1) Ensure 'Maximum Auto-Lock' is set to '2 minutes' or less (Scored)....	133
3.4.4 (L1) Ensure 'Maximum grace period for device lock' is set to 'Immediately' (Scored) .....	135

3.4.5 (L1) Ensure 'Maximum number of failed attempts' is set to '6' (Scored) ....	137
3.5 VPN .....	139
3.5.1 (L1) Ensure 'VPN' is 'Configured' (Not Scored) .....	139
3.6 Mail .....	141
3.6.1 (L1) Ensure 'Allow user to move messages from this account' is set to 'Disabled' (Scored) .....	141
3.6.2 (L2) Ensure 'Allow Mail Drop' is set to 'Disabled' (Scored) .....	143
3.7 Notifications .....	145
3.7.1 (L1) Ensure 'Notification Settings' are configured for all 'Managed Apps' (Scored) .....	145
3.8 Lock Screen Message .....	147
3.8.1 (L1) Ensure 'If Lost, Return to... Message' is 'Configured' (Not Scored) .....	147
4 Additional Recommendations .....	149
4.1 (L1) Ensure device is not obviously jailbroken (Scored) .....	150
4.2 (L1) Ensure 'Software Update' returns 'Your software is up to date.' (Scored) .....	152
4.3 (L1) Ensure 'Automatic Downloads' of 'App Updates' is set to 'Enabled' (Scored) .....	154
4.4 (L1) Ensure 'Find My iPhone/iPad' is set to 'Enabled' on end-user owned devices (Scored) .....	156
4.5 (L2) Ensure the latest iOS device architecture is used by high-value targets (Not Scored) .....	158
Appendix: Summary Table .....	159
Appendix: Change History .....	163



# Overview

This document, *Security Configuration Benchmark for Apple iOS 13 and iPadOS 13*, provides prescriptive guidance for establishing a secure configuration posture for the Apple iOS and iPadOS version 13. This guide was tested against the Apple iOS 13.2 and iPadOS 13.2 and using Apple Configurator v2.11.1. This benchmark covers the Apple iOS 13 and iPadOS 13 on all supported devices. As of the publication of this guidance, devices supported by iOS 13 or iPadOS 13 include the following:

- iPhone 6s and later
- iPod touch (7th generation) and later
- iPad Pro and later
- iPad (5th generation)
- iPad Air 2
- iPad mini 4 and later

In determining recommendations, the current guidance consider iOS and iPadOS devices as having the same use cases and risk/threat scenarios. In all but a very few cases, configuration steps, default settings, and benchmark recommended settings are identical regardless of hardware platform or operating system; for the few cases where variation exists, the benchmark notes the difference within the respective section. To obtain the latest version of this guide, please visit <http://cisecurity.org>. If you have questions, comments, or have identified ways to improve this guide, please write us at [support@cisecurity.org](mailto:support@cisecurity.org).

## Intended Audience

This document is intended for system and application administrators, security specialists, auditors, help desk, end users, and platform deployment personnel who plan to use, develop, deploy, assess, or secure solutions that incorporate the Apple iOS 13 or iPadOS 13.

## Consensus Guidance

This benchmark was created using a consensus review process comprised of subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been published. During this phase, all feedback provided by the

Internet community is reviewed by the consensus team for incorporation in the benchmark. If you are interested in participating in the consensus process, please visit <https://workbench.cisecurity.org/>.

**3.2.1.4 (L1) Ensure 'Allow iCloud backup' is set to 'Disabled' (Scored)****Profile Applicability:**

- Level 1 - Institutionally Owned Devices

**Description:**

This recommendation pertains to allowing iCloud backup.

**Rationale:**

iCloud backups are encrypted in transit and at rest within Apple's infrastructure, but there is no protection against restoring a backup to an unmanaged device. This allows for data leakage.

**Audit:**

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, verify that under the tab `Functionality`, that the checkbox for `Allow iCloud backup` is unchecked.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `iCloud backup not allowed` is displayed.

**Remediation:**

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, under the tab `Functionality`, uncheck the checkbox for `Allow iCloud backup`.
5. Deploy the Configuration Profile.

**CIS Controls:**

Version 6

14 Controlled Access Based on the Need to Know

Controlled Access Based on the Need to Know

Version 7

13.4 Only Allow Access to Authorized Cloud Storage or Email Providers

Only allow access to authorized cloud storage or email providers.

### 3.2.1.5 (L1) Ensure 'Allow iCloud documents & data' is set to 'Disabled' (Scored)

#### Profile Applicability:

- Level 1 - Institutionally Owned Devices

#### Description:

This recommendation pertains to the storage and sync of data through iCloud from institutionally owned devices.

#### Rationale:

Institutionally owned devices are often connected to personal iCloud accounts. This is expected and normal. The data from institutionally owned devices though should not co-mingle with the end-user's personal data. This poses a potential avenue of data leakage.

#### Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, verify that under the tab `Functionality`, that the checkbox for `Allow iCloud documents & data` is unchecked.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Documents in the Cloud not allowed` is displayed.

#### Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, under the tab `Functionality`, uncheck the checkbox for `Allow iCloud documents & data`.

5. Deploy the Configuration Profile.

**CIS Controls:**

Version 6

14 Controlled Access Based on the Need to Know

Controlled Access Based on the Need to Know

Version 7

13.4 Only Allow Access to Authorized Cloud Storage or Email Providers

Only allow access to authorized cloud storage or email providers.